FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272294-0

Total Deleted Page(s) = 13
Page 11 ~ b3; b7E;
Page 12 ~ b1; b3; b7E;
Page 30 ~ b1; b3; b7E;
Page 31 ~ b1; b3; b7E;
Page 32 ~ b1; b3; b7E;
Page 33 ~ b1; b3; b7E;
Page 34 ~ b1; b3; b7E;
Page 35 ~ b1; b3; b7E;
Page 36 ~ b1; b3; b7E;
Page 37 ~ b1; b3; b7E;
Page 38 ~ b1; b3; b7E;
Page 40 ~ b1; b3; b7E;
Page 41 ~ b1; b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FBI

[Component Seal]

Privacy Impact Assessment
for the
Foreign Terrorist Tracking Task Force/National Security Analysis Center (FTTTF/NSAC)

Issued by:

Reviewed by: Luke J. McCormack, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [Component to insert date of PIA approval]

(March 2012 DOJ PIA Form)

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Office: Phone: Bldg./Room Number: Email:	**PIA AUTHOR** (if different from POC) Name: Office: Phone: Bldg./Room Number: Email:
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Office: Phone: Bldg./Room Number: Email: Signature: _____ Date signed: _____	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: Office: Phone: Bldg./Room Number: Email: Signature: _____ Date signed: _____

DOJ PIA REVIEWING OFFICIAL Chief Information Officer Department of Justice (202) 514-0507 Signature: _____ Date signed: _____	**DOJ PIA APPROVING OFFICIAL** Nancy C. Libin Chief Privacy and Civil Liberties Officer, ODAG Department of Justice (202) 307-0697 Signature: Nancy C. Libin Date signed: 8/23/12

(U) Privacy Impact Assessment
for the

(U) Foreign Terrorist Tracking Task Force/National Security Analysis Center (FTTTF/NSAC)

August 11, 2008

(U) Contact Point
Section Chief (SC) John A. Boyle
FTTTF/NSAC
Federal Bureau of Investigation
(703) 553-7990

(U) Reviewing Official
David C. Larson
Privacy and Civil Liberties Officer
Federal Bureau of Investigation

(U) Approving Official
Kenneth Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 353-8878

(U) Introduction

(U) The National Security Branch (NSB) of the Federal Bureau of Investigation (FBI) consists of the Counterterrorism Division (CTD), Counterintelligence Division (CD), the Directorate of Intelligence (DI) and the Weapons of Mass Destruction Directorate (WMDD) and was created in September 2005, to carry out the mandate of a June 2005 Presidential Directive that a National Security Service be created within the FBI.

(U) Following an assessment of the NSB and its components, FBI leadership recommended that a National Security Analysis Center (NSAC) be created to support NSB components in the detection, identification, tracking, and assessment of individuals and entities that pose threats to the United States and its interests. The vision of the NSAC is that it is to become the NSB's center of excellence for specialized analysis of data and information regarding threats to national security. FBI leadership recommended that existing analytical and technological capabilities of the Foreign Terrorist Tracking Task Force (FTTTF) be leveraged to fill vital intelligence and analytical needs of the NSB. While FTTTF's mission has focused on locating foreign terrorists, its architecture and business processes are scalable and can be used to support the NSAC.

(U) NSAC capabilities therefore will build upon the FTTTF System that was described in the previous Privacy Impact Assessment (PIA) for FTTTF. This PIA subsumes the previous FTTTF PIA (66F-HQ-C1321794 Serial 213, 10/17/2005) and its addenda (66F-HQ-C1321794 Serial 307, 9/14/2006; 190-HQ-C1321794 Serial 368, 6/25/2007). This PIA will refer to both systems in the singular as the FTTTF/NSAC "system," commonly referred to as the Datamart.

(U) This Datamart has been identified to support NSAC operations because, as has been demonstrated with FTTTF, it provides access to relevant information and best meets the needs of the FBI to conduct the tactical and strategic analyses necessary to mitigate threats to national security. NSAC will utilize existing FTTTF business processes, but expand the scope of FTTTF analytical capabilities by adding new datasets and engaging in analysis for additional mission-related purposes. Because of this expansion, the privacy risks previously described in the FTTTF PIA have changed or new risks have been identified.[1] This PIA will describe those changes and how any new risks have been mitigated. Any further changes to the NSAC that necessitate a revision in this PIA will cover FTTTF as well, since both are built on the same information technology foundation.

[1] (U)The FBI Privacy and Civil Liberties Officer has also approved the addition of datasets for FTTTF/NSAC that will contribute to the mission of NSAC. This approval is documented in a separate communication to FTTTF/NSAC (319X-HQ-A1487720 Serial 453, 7/30/2008. The additional datasets are described in Appendix A (2).

(U) Section 208 of the E-Government Act of 2002, P.L. 107-347, requires that agencies conduct PIAs on information technology systems that collect and maintain identifiable information regarding individuals, but exempts national security systems from the PIA requirement.[2] The current FTTTF system is a national security system, and is therefore exempt from the section 208 requirement, and the NSAC similarly meets the requirements for designation as a national security system. Nevertheless, as a matter of policy, both the Department of Justice (DOJ) and the FBI require PIAs for national security systems. Accordingly, this PIA is conducted pursuant to DOJ and FBI PIA Guidelines. Because it builds upon the previous PIA covering the FTTTF Datamart, it encompasses the FTTTF Datamart as currently configured. As changes are made in the Datamart to support NSAC and, as appropriate, FTTTF operations, this PIA will be reviewed and revised.

Section 1.0
(U) The System and the Information Collected and Stored within the System.

1.1 (U) What information is to be collected?

(U) NSAC, like FTTTF, will aggregate datasets that are currently available from within the FBI and externally from other agencies, into a Datamart where the information can be queried in response to taskings from the NSB and its component divisions. The precise configuration of the Datamart is sensitive law enforcement information, but in general, the datasets are information collections that have a nexus to the national security interests of the United States. The Datamart is a dynamic system: the data is continuously updated or deactivated and archived based on an assessment of mission needs and requirements.

(U) Some of the datasets currently available,[3] which are obtained primarily from

b3
b7E

[2] (U) No PIA is required for national security systems as defined at 40 U.S.C. §11103. National security systems are defined as information systems operated by the Federal government, the function, operation, or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons system, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative or business applications, such as payroll, finance, logistics, and personnel management.

[3] (U) The datasets that have been preliminarily identified for use are listed in Appendix A.

[redacted] b3 b7E

(U) [redacted] b3 b7E

[redacted] b3 b7E

(U) The specific identifiers available from each of the datasets vary, but at a minimum most can be expected to contain personally identifiable information such as name, including variations, date and place of birth (if available), and unique numbers such as alien registration number and/or Social Security number. [redacted] b3 b7E

1.2 (U) From whom is the information collected?

(U) The majority of the datasets, which are currently maintained in the FTTTF Datamart and which will be used by NSAC, are from interagency government sources, including the FBI.[4] FTTTF and NSAC employees are not first line intelligence collectors or investigators and, therefore, do not collect personal information directly from individuals. All of the datasets have been, and will continue to be, acquired based upon specific mission needs. In addition, NSAC

[4] See Appendix A.

and FTTTF will query commercial data sources and aggregate the results, as appropriate, with government data to support analytical operations.

Section 2.0
(U) The Purpose of the System and the Information Collected and Stored within the System.

2.1 (U) Why is the information being collected?

(U) The FTTTF Datamart has been used to provide information to detect the presence of or locate known or suspected terrorists within the U.S. or those attempting to gain entry into the U.S. Carrying out this mission requires timely and complex analyses that involve the evaluation of pertinent government data, supplemented with public source information and/or commercial data relevant to the FTTTF mission. NSAC will utilize the Datamart and business processes of the FTTTF in order to support NSB components in the detection, identification, tracking, and assessment of individuals and entities that pose threats to the United States and its interests.

2.2 (U) What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

(U) The following authorities form the legal foundation:

28 U.S.C. 533, which authorizes the FBI to investigate violations of federal law, including acts of terrorism (18 U.S.C. 2332b), for which the FBI has primary investigative jurisdiction;

28 U.S.C. 534, which authorizes the FBI to collect and retain identification, criminal information, crime, and other records;

28 C.F.R. 0.85, which authorizes the FBI to conduct federal criminal investigations and to exercise lead agency responsibility in counterterrorism investigations;

HSPD-2, 6, and 11, all of which direct the strengthening of screening and analysis programs to detect, identify, and interdict individuals entering or already within the United States who pose a terrorist threat to national security. HSPD-2 specifically directs the FTTTF to perform this function;

(U) The Attorney General Guidelines for Domestic FBI Operations (AGG-Dom), Part II authorizes the FBI to carry out investigations to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2.3 (U) Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

(U) Privacy risks include the risk of breach in the process of obtaining the datasets that comprise the Datamart; internal or external threats once the data is collected; the risk the information, by itself or in combination with other data, may not be accurate or timely; and the risk of improper access to the data or misuse of the information once the data is obtained.

[redacted] b3 b7E

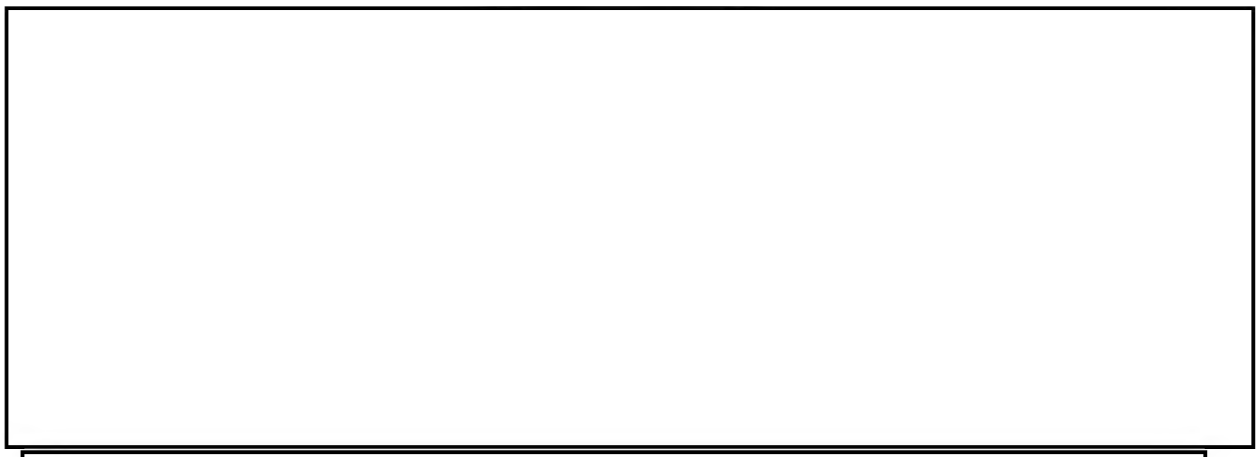
(U) The risk of a data breach is also mitigated by the procedures and safeguards put in place for granting and revoking access to the data. End user access to the Datamart as well as access to the technical interface is strictly controlled. Access to the Datamart is not FBI-wide; it is limited to designated users assigned to FTTTF/NSAC and other users on case-by-case basis. An authorization policy exists to restrict the access to the following controlled elements: datasets, folders, searches and other elements of the system. The access policy determines which individuals have access to the aforementioned controlled elements.

(U) In addition to the protections that mitigate the risk of logical breaches, FTTTF and NSAC also have protections to mitigate the risk of physical breaches. Physical access to the work space and the servers in the data center are even further restricted.

(U) Risk is also mitigated by auditing. All users know they are subject to periodic, random auditing of what was searched, when, and by whom. Moreover, account access is also subject to periodic, random auditing.

(U) Additionally, to meet Federal Information Security Management Act (FISMA) requirements, all FBI systems are Certified and Accredited in accordance with the FBI Certification and Accreditation Handbook and DOJ Policy 2640.2E, Information Technology Security.

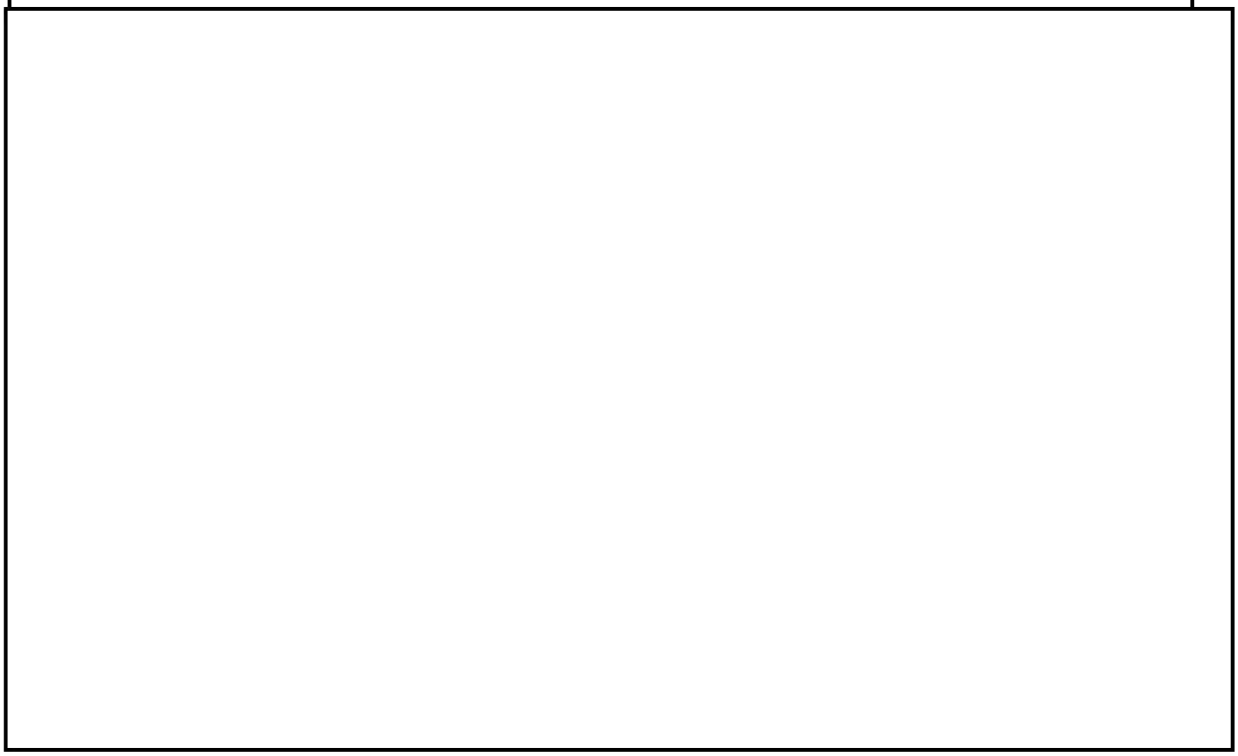
(U) The system resides in a secure facility with appropriate password authentication and other protections. [redacted] b3 b7E The FTTTF continues to improve operational readiness and is engaged in contingency planning as well as Continuity of Operations (COOP) initiatives.



(S)

b1
b3
b7E

b3
b7E



b3
b7E

(U) In addition, the FBI Nondisclosure Agreement is signed by all vendors and FBI security policies are followed to safeguard all information technology assets, including the FTTTF system. Access to the system is restricted under established security access controls. FTTTF and NSAC analysts are trained in the appropriate use and access of the data. For example, accessing the FTTTF/NSAC system for personal use is prohibited and subject to severe

penalties including termination of employment. All queries in the FTTTF/NSAC system are recorded so that effective auditing can be accomplished. Handling instructions are kept for every dataset and the reminders are embedded in the system interface for ease of use. Analysts are also provided periodic refresher training.

(U) Moreover, the addition of any new datasets to the FTTTF/NSAC system, as well as any proposals to access additional commercial data providers and/or datasets, must be reviewed and approved by the FBI Privacy and Civil Liberties Officer to ensure that privacy concerns are addressed.

Section 3.0
(U) Uses of the System and the Information.

3.1 (U) Describe all uses of the information.

(U) The information from the Datamart is used to respond to predicated individual or batch queries that are derived from official government requests or leads based on law enforcement, intelligence, or counterterrorism-related investigative activity. The results will be used to support the strategic and analytic needs of the NSB and its mission, allowing the NSB to respond to intelligence-based threats and more effectively to identify, track, and coordinate actions regarding subjects of investigative interest and to provide support services across NSB mission areas. In particular, FTTTF/NSAC will use the Datamart to support NSB components in the detection, identification, tracking, and assessment of individuals and entities that pose threats to the United States and its interests. Where appropriate, FTTTF/NSAC will also share query results and intelligence products with external agencies.

(S)

b1
b3
b7E

(U) The query results are returned to NSB for further action as appropriate.

3.4 (U) What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

(U) The retention schedule for data in NSAC mirrors the retention schedule approved for the FTTTF Datamart. A copy of the retention schedule is attached as Appendix B.

3.5 (U) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.

(U) Strong audit controls and robust training are used to ensure that information is handled as described above. All queries in the system are recorded and subject to random auditing in which checks are conducted to validate user queries and/or to search for anomalous activity. In addition, FTTTF/NSAC has a quarterly audit policy to ensure that employees have the appropriate level of access to the datasets, as well as to ensure access is terminated for employees who leave FTTTF/NSAC or no longer require access to particular datasets. Supervisors exercise oversight over analysts' work and all finished products are made part of the FBI's case management system.

b3
b7E

(U) Access to the system is also predicated on having appropriate approval and verification of security credentials by security personnel. Information Systems Security Officers are present onsite and monitor logical access for both internal and external attacks on the system. In addition, all individuals with access to the system execute non-disclosure agreements, which prohibit the unauthorized access and/or disclosure of the data. The system resides in a secure facility where physical access is strictly controlled. Additionally, handling instructions are kept for every dataset and reminders are embedded in the system interface for ease of use. FTTTF and NSAC analysts are also provided initial and periodic refresher training.

Section 4.0
(U) Internal Sharing and Disclosure of Information within the System.

4.1 (U) With which internal components of the Department is the information shared?

(U) The only DOJ component that has access to the information in the FTTTF/NSAC system is the FBI, including FBI personnel and contractors. These individuals hold security clearances, receive indoctrination and training, and sign appropriate non-disclosure agreements and other access documentation prior to gaining access to the data. Access is regulated, maintained, and documented by system administrators. Authorized FTTTF and NSAC personnel have the capability to and so restrict user access when necessary.

4.2 (U) For each recipient component or office, what information is shared and for what purpose?

(U) The information is accessed as described above and resulting tactical intelligence products and case leads are provided to authorized recipients. Management reviews and approves products prior to dissemination.

4.3 (U) How is the information transmitted or disclosed?

b3
b7E

4.4 (U) Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

(U) As explained in response to question 2.3, one privacy risk is that the data may be accessed or used inappropriately. Strong mitigation measures are in place to prevent this from happening. The FTTTF and NSAC policies and procedures, as implemented, require authorized personnel to control access to the data. Management must review and approve any disclosure of query results from the FTTTF or NSAC. All queries in the system are recorded so that effective auditing can be conducted. Furthermore, all individuals with access to the system execute non-disclosure agreements, which prohibit the unauthorized disclosure of the data. The FTTTF has a

quarterly audit policy to ensure that employees have the appropriate level of access to FTTTF data, as well as to ensure access is terminated for employees who leave FTTTF or no longer require access to particular datasets. In addition to FTTTF/NSAC audit procedures, the FTTTF and NSAC continue to work with the FBI Security Division to ensure compliance with all FBI required monitoring, audit procedures, and policies. FTTTF/NSAC utilizes periodic, random auditing to validate user queries.

(U) The system resides in a secure facility with appropriate password authentication and other protections. [redacted] The FTTTF/NSAC continues to improve operational readiness and is engaged in contingency planning as well as continuity of operations (COOP) initiatives.

b3
b7E

[redacted]

b3
b7E

Section 5.0
(U) External Sharing and Disclosure

5.1 (U) With which external (non-DOJ) recipient(s) is the information shared?

(U//FOUO) FTTTF/NSAC co-located partners, such as Department of Homeland Security (DHS), Immigration Customs Enforcement (ICE), DOD Counter Intelligence Field Activity (CIFA), Financial Crimes Enforcement Network (FinCEN), Transportation Security Administration (TSA), and the Central Intelligence Agency (CIA), provide datasets ingested into the Datamart and their detailees have access to the Datamart itself.

(U//FOUO) In addition to sharing with these co-located partners, FTTTF/NSAC also receives datasets from other federal agency contributors. In accordance with the terms of MOUs with both categories of data contributors, FTTTF and NSAC return the results of analyses that are pertinent to the mission and authority of these data contributors. While the primary mission of NSAC will be to support the analytical requirements of the FBI's NSB, because some of the datasets to be used by NSAC will come from these entities, it is anticipated that NSAC will share appropriate intelligence products and query results with these other agencies.

[redacted]

b3
b7E

b3
b7E

5.2 (U) What information is shared and for what purpose?

(U//FOUO) In any analytical product the following information may be shared if appropriate and authorized: identity and biographical data; threat assessments; and other information obtained from open sources, third party information and FBI files. These analytical products are either in direct support of FBI investigations and/or intelligence sharing initiatives.

5.3 (U) How is the information transmitted or disclosed?

b3
b7E

(U//FOUO) Additionally, information may be provided to FBI HQ support entities (Field Offices and Legats), that may, as appropriate, disseminate to external entities other than the aforementioned FTTTF/NSAC partners through approved FBI dissemination procedures.

5.4 (U) Are there any agreements concerning the security and privacy of the data once it is shared?

(U) FTTTF has executed MOUs for data received from Task Force Partners, who are co-located with FTTTF, as well as with other federal agency data contributors. FTTTF is restricted in how it uses data, pursuant to the MOU with the particular data provider. FTTTF has ensured that users are aware of and trained on such issues. The MOUs have been sent for inclusion to the Office of General Counsel (OGC) Law Library.[6] Current MOUs are being reviewed and it is anticipated that certain MOUs will need to be updated prior to certain data being utilized for NSAC operations.

(U) When analytical products are shared, FTTTF and NSAC expressly relate to the recipient(s) how the information may be disseminated and if there are any caveats.

[6] (U) Please see referenced EC 319T-HQ-A1487667-CTD Serial 1652.

5.5 (U) What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

(U) Prior to gaining access to the system, FTTTF and NSAC ensure that **all** individuals are cleared, receive indoctrination and training, and sign appropriate non-disclosure agreements and other access documentation. Access is regulated, maintained, and documented by system administrators. The FTTTF and NSAC have the ability to restrict user access and have restricted access in certain cases.

(U) Participating agencies agree to use the data only for legitimate investigative and intelligence purposes. Handling instructions are kept for every dataset and reminders are embedded in the system interface for ease of use. FTTTF and NSAC analysts are also provided periodic refresher training.

(U) However, for those external users that do not have actual access to the system, but receive access to the analytic products, FTTTF and NSAC expressly relate to the recipient(s) how the information may be disseminated and if there are any caveats.

5.6 (U) Are there any provisions in place for auditing the recipients' use of the information?

(U) Yes. The same mechanisms utilized for internal users are utilized for auditing external usage for those that have access to the system. All queries are recorded so effective auditing can be conducted. Furthermore, the non-disclosure agreements prohibit the unauthorized disclosure of the data. The FTTTF has a quarterly audit policy to ensure that users have the appropriate level of access to FTTTF data, as well as to ensure access is terminated for users who leave FTTTF or no longer require access to particular datasets. NSAC employs these same measures. In addition to FTTTF/NSAC audit procedures, the FTTTF and NSAC continue to work with the FBI Security Division to ensure compliance with all FBI required monitoring, audit procedures, and policies.

(U) There are no means to audit the use of analytical products that are provided to external users that do not have access to the system. However, all disseminated products will be marked with the appropriate caveats and are required to be handled accordingly by external users.

5.7 (U) Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

(U) A privacy risk that arises from external sharing is that the data has the potential to be misused. This risk is mitigated in several ways. All queries in the system are recorded so effective auditing can be conducted. Furthermore, all individuals with access to the system, including agency task force members, execute non-disclosure agreements which prohibit the unauthorized disclosure of the data. The FTTTF has a quarterly audit policy to ensure these individuals have the appropriate level of access to data, as well as to ensure access is terminated for employees and task force members who leave FTTTF and/or no longer require access to particular datasets. NSAC adheres to these same practices. In addition to FTTTF/NSAC audit procedures, the FTTTF and NSAC continue to work with the FBI Security Division to ensure compliance with all FBI required monitoring, audit procedures, and policies. FTTTF and NSAC utilize a periodic, random auditing in which data checks are conducted to validate user queries.

(U) Every dataset has a data dictionary, which describes if the information is to be shared, how the data can be shared, as well as any security caveats and a point of contact for any questions, including privacy or release questions. Additionally, the MOU or Agreement is available for view by the user when they are logged-into the system.

(U) In addition to the caveats mentioned in the data dictionary, all disseminated analytical products will be marked with the appropriate caveats and are required to be handled accordingly by external users.

	(S) b1 b3 b7E
	b3 b7E

b3
b7E

Section 6.0
(U) Notice

(U) The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 (U) Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

(U//FOUO) According to their policies and procedures, the original providers of the data may or may not provide notice to individuals that the data collected may be shared with law enforcement. Individual notice is not provided by FTTTF/NSAC. The FTTTF/NSAC system is used for law enforcement and national security purposes. Providing individuals with a notice and opportunity to consent could jeopardize on-going investigations as well as compromise intelligence sources and/or methods. The FBI has published a Privacy Act System of Records Notice (SORN) for FBI's investigative records, which provides general notice regarding entities with which and situations when the FBI may share its investigative and intelligence records.

6.2 (U) Do individuals have an opportunity and/or right to decline to provide information?

(U) See 6.1 Above.

6.3 (U) Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

(U) See 6.1 Above.

6.4 (U) Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

(U) FTTTF/NSAC does not provide notice to individuals whose information is collected in the Datamart, which is a privacy risk. The FBI has published a Privacy Act System of Records Notice (SORN) for the Data Warehouse System (JUSTICE/FBI-022), which covers the FTTTF/NSAC Data Mart. This SORN provides general notice regarding entities with which and situations when the FBI may share its investigative and intelligence records. The FBI's routine uses for this system provide further notice of the ways in which information collected by the FBI is shared. These notices, therefore, help to mitigate the privacy risk.

Section 7.0
Individual Access and Redress

7.1 (U) What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

(U) Applicable regulations found in 28 CFR Part 16, Subparts A and D, which have been issued pursuant to the Freedom of Information and Privacy Acts, govern requests for access to information in FBI files.

7.2 (U) How are individuals notified of the procedures for seeking access to or amendment of their information?

(U) 28 C.F.R. 16.41 and 16.46 provide information on individual access and amendment of FBI records. Amendment of FBI records is a matter of discretion as the records are exempt from the Privacy Act amendment provisions.

7.3 (U) If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

(U) See previous response.

7.4 (U) Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

(U) As a general matter, although FBI records are exempt from Privacy Act access and amendment procedures, the FBI strives to maintain accurate information and will, in its discretion, consider amendment requests. If an individual wishes to contest information, it is likely to be because an investigation was conducted on the basis of analytical information received from FTTTF/NSAC. Amendment or correction of the investigatory information to the extent that it is available, rather than of the FTTTF/NSAC information, would provide any necessary redress. Amendment or correction of data submitted by other agencies is governed by the rules of those agencies. However, pursuant to the DOJ Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment (ISE), FBI will communicate potential errors or deficiencies in the data to the other's agency's ISE Privacy official.

Section 8.0
(U) Technical Access and Security

(U) The following questions are intended to describe technical safeguards and security measures.

8.1 (U) Which user group(s) will have access to the system?

(U) Various technical and analytical entities have access to the multiple elements (datasets, query requests, folders, and search results) of the system based upon their mission requirements. Prior to any additional user groups being established, they must receive approval from FTTTF/NSAC management based upon the established policy guidelines.

8.2 (U) Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

(U) Only authorized personnel, including contractors and other government agency task force members, have access to the information in the FTTTF/NSAC system. These individuals are cleared, receive indoctrination and training and sign appropriate non-disclosure agreements and other access documentation prior to gaining access to the data. Access is regulated,

maintained and documented by system administrators. The FTTTF/NSAC has the ability to restrict user access.

8.3 (U) Does the system use "roles" to assign privileges to users of the system?

(U) Yes. The application supports the assignment of privileges and accesses to users based upon the user group and functional "role." Three functional roles are currently in use: General User, System Administrator, and Data Librarian.

(U) New user groups are set up according to their data needs and functions. Prior to being established, new user groups go through an approval process in conformity with the standard operating procedure relating to system access.

8.4 (U) What procedures are in place to determine which users may access the system and are they documented?

(U) New system accounts are created through the FTTTF/NSAC New User INDOC process. Account creation, modification and deletion are fully documented with approvals granted by the respective Unit Chiefs or their designated representatives for FTTTF/NSAC analysts. Signed approvals are kept on file with the FTTTF Operational Support Unit.

(U//FOUO) The system is used primarily by FTTTF analytical units. There are users from other organizations,[7] however, and the access privileges for the different user groups are not the same. Usage is split between users on the FBI Secret Enclave (FBISE) and the unclassified enclave. Because the number of users and their access privileges must be carefully controlled, procedures for creating, modifying and disabling accounts are strictly followed.

(U) ECs document the different access privileges to the system for the respected entities.

(S)

b1
b3
b7E

8.5 (U) How are the actual assignments of roles and rules verified, according to established security and auditing procedures?

(U) An FTTTF/NSAC working group developed the process for verifying the established security and auditing procedures.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

(U) The system software application performs transactional auditing. Audit logs are available online for 90 days and are then archived to tape and maintained according to established FBI requirements. In addition to the software application audits, all queries in the system are recorded and subject to random auditing in which checks are conducted to validate user queries and/or to search for anomalous activity. In addition, FTTTF/NSAC has a quarterly audit policy to ensure that employees have the appropriate level of access to the datasets, as well as to ensure access is terminated for employees who leave FTTTF/NSAC or no longer require access to particular datasets.

8.7 (U) Describe what privacy training is provided to users, either generally or specifically relevant to the functionality of the program or system?

(U) Only authorized personnel, including contractors and other government agency task force members, have access to the information in the FTTTF/NSAC system. These individuals are cleared, receive indoctrination and training and sign appropriate non-disclosure agreements and other access documentation prior to gaining access to the data. Access is regulated, maintained, and documented by system administrators. The FTTTF and NSAC have the ability to restrict user access and they do so as needed in certain cases.

8.8 (U) Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

(U) The system and software application were reaccredited at the UNCLASSIFIED level as of April 29, 2008. Additionally, the software application is accredited at the SECRET level as part of the FBISE system as of August 8, 2005, and is in the process of being reaccredited.

8.9 (U) Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

(U) Privacy risks from this system stem from improper access and inadequate security. These risks have been mitigated in several ways. All queries in the system are recorded so effective auditing can be conducted. Furthermore, all individuals with access to the system execute non-disclosure agreements which prohibit the unauthorized disclosure of the data. The FTTTF/NSAC has a quarterly audit policy to ensure that employees have the appropriate level of access to the data, as well as to ensure that access is terminated for employees who leave FTTTF or NSAC or no longer require access to particular datasets. The FTTTF/NSAC continuously works with the FBI Security Division to ensure compliance with all required monitoring, audit procedures, and policies. In addition, FTTTF/NSAC has a random auditing program in which periodic checks are conducted to validate user queries.

(U) The data system resides in a secure facility with appropriate password authentication and other protections. [redacted] Access to the system is controlled under established security access controls to cleared personnel only. The system is managed and updated by assigned and cleared information technology specialists. In addition, the FTTTF continues to improve operational readiness and is engaged in contingency planning as well as COOP initiatives.

b3
b7E

(U//FOUO) As the system resides in a secure FBI facility, users need physical access to FBI Secret Enclave to access the Datamart. Once an employee's access to the facility and the Secret Enclave has been terminated, access to the Datamart is terminated as well. For internal users, FTTTF/NSAC out-processing procedures require that Datamart accounts are terminated immediately upon the employee departure. For external users, i.e., those users who are not physically located at the FTTTF/NSAC facility, policy requires that FTTTF be notified when accounts are no longer valid. To further enhance security measures, an audit policy has been implemented to ensure that accounts which are not in use are terminated.

Section 9.0
(U)) Technology

9.1 (U) Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

(U) Yes. From 2002 forward, FTTTF has reviewed various hardware and software technologies to determine which components meet system requirements at affordable prices. Some components were selected for compatibility with the existing enterprise architecture. For technology refresh, new technologies and vendors continue to be evaluated.

9.2 (U) Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

(U) Data integrity, privacy, and security were, and continue to be, important in the design of the FTTTF/NSAC system. As each new feature or change is made to the FTTTF/NSAC system to suit new requirements, it is analyzed for any effects on integrity, privacy, and security. A separate development group provides independent analysis of these factors. Technical changes to the FTTTF/NSAC system must be approved by a Technical Review Board, which includes a review by the information assurance officers. Data acquisition and its impact on privacy are also reviewed in-house and then analyzed and approved by the FBI Privacy and Civil Liberties Officer. A privacy attorney has been assigned to NSAC to provide onsite assistance in analyzing the privacy impacts of decisions made for and about the system.

(U) As a result of our analyses the following technical decisions were made to achieve these goals:

	b3 b7E
	b3 b7E

When users enter query information or annotate the data in the Datamart, they are required to select the appropriate classification for the information and can mark it with caveats.

(U) At a policy level, the use of the various data in the FTTTF/NSAC system is governed by the MOUs and agreements which have been established with the providers of the data. These agreements are documented in the FTTTF/NSAC system itself. Specific handling restrictions on the different datasets are prominently displayed both in the detailed description of the dataset as well as in reports that include particular records from the dataset. Training emphasizes the user's role in maintaining the security of the data. The training points out that Datamart contents are copies of data from other systems, and the originating agency or organization should be consulted for the most accurate, up-to-date information.

(U) For operations and maintenance of the FTTTF/NSAC system, the administrators allowed to access the servers storing and operating the data are limited in number. All staff performing these operations must sign privileged user agreements and have a final Top Secret security clearance.

9.3 (U) What design choices were made to enhance privacy?

(U) The major design choice was to create a Datamart in order to best meet the analytical needs of the FTTTF/NSAC. Recognizing that ingesting data may mean that data owner changes may not be made to the Datamart in real time, FTTTF/NSAC has focused on training its analysts to use multiple sources to verify information and to set leads for investigators to further confirm the data results.

(S)

b1
b3
b7E

(U) Conclusion

(U) Because of the successful use of technology by the FTTTF to track foreign terrorists, a decision was made to leverage the existing FTTTF architecture and business processes to fill intelligence and analytical needs for the NSB. The privacy risks attendant to the development of the NSAC primarily stem from the choice of architecture and from risks arising from data inaccuracy and misuse. These risks have been carefully addressed through strong audit controls that will detect inappropriate use of the system and other anomalies, robust training for all users on both the privacy and security aspects necessary for use of the system [redacted] b3 b7E [redacted] In addition, NSAC employs a full-time privacy counsel to provide legal advice on use of the system. Finally, all data ingested into the system has been approved by the FBI Privacy and Civil Liberties Officer. Moreover, any future system changes that impact privacy, as well as the inclusion of any additional datasets will also be reviewed and approved by the FBI Privacy and Civil Liberties Officer.

(U) Responsible Official

SC John A. Boyle

FTTTF/NSAC

703-553-7903

8/12/2008

Date

(U) Approval Signatures

_____ 8/27/2008

David C. Larson

Date

Privacy and Civil Liberties Officer
Federal Bureau of Investigation

_____ _____

Kenneth Mortensen

Date

Chief Privacy Officer and Civil Liberties Officer
Department of Justice

Appendix A: (U) Datasets Used in the FTTTF/NSAC Datamart

(U) What follows are two lists of datasets: (1) Datasets Approved in the Previous FTTTF Privacy Impact Assessment and Its Respective Addendums and (2) Additional Datasets That Are Now Approved for Use in the FTTTF/NSAC Datamart. These two lists combined encompass the entire roster of datasets currently in the FTTTF/NSAC Datamart. As stated in previously, FTTTF and NSAC intend that the ingestion of additional datasets will be subject to approval by the FBI Privacy and Civil Liberties Officer of the General Counsel.

Both lists are classified SECRET//NOFORN in their entirety since when combined with the procedures and methods within the aggregate of this document, the information could lead to a determination that a particular individual is or may be a terrorist or supporter of international terrorism

(U)

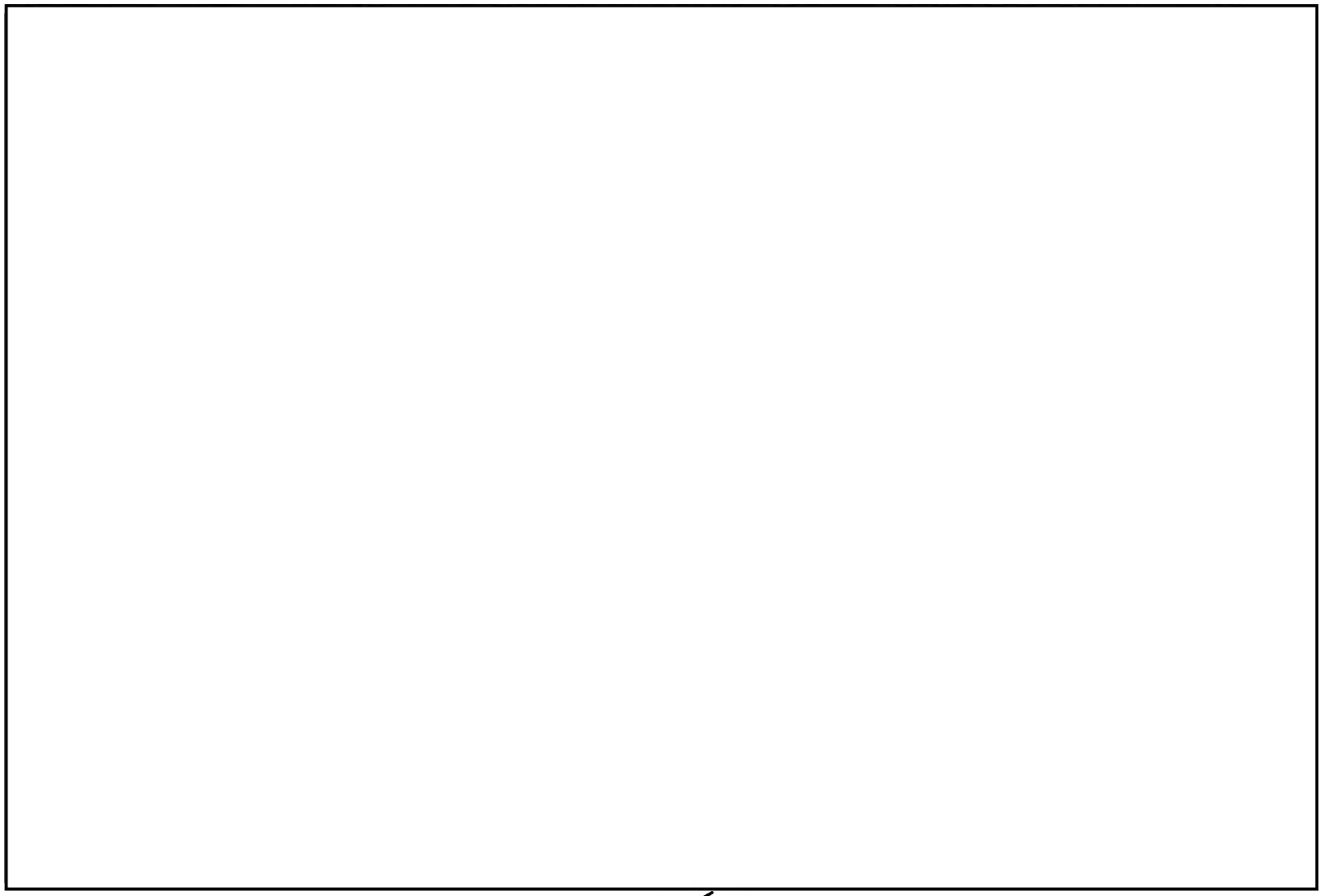
A. (1) (~~SECRET~~//NOFORN) Datasets Approved in the Previous FTTTF Privacy Impact Assessment and Its Addendums

(S)

b1
b3
b7E

(U)

A. (2) (~~SECRET~~//NOFORN) Additional Datasets That Are Now Approved for Use in the FTTTF/NSAC Datamart



(S)

b1
b3
b7E

Appendix B (U) Foreign Terrorist Tracking Task Force DataMart Retention Schedule

(U) Background:

1. (U) Inputs: The FTTTF data mart is populated with data from the FBI, other federal government agencies, and from other non-federal government sources.

a. (U) Data from the FBI and other government agencies' systems: The official record is maintained within other FBI record systems and/or other government agency systems. Copies of records are uploaded into FTTTF to facilitate data matching and analysis.

b. (U) Data from non-federal sources: These data sources are queried remotely, and the results of the query are ingested into the FTTTF data mart for analysis.

(U) Disposition: DELETE/DESTROY 180 days after verification of successful uploading into the data mart or when superseded by more current data, whichever is sooner.

2. (U) Data Files: The "data mart" contains a variety of data sets and related metadata, including copies of FBI and other government agency records, as well as data from non-federal sources.

a. (U) Data from FBI and other government agencies' systems: The record copy is managed in the system of origin for legal, fiscal, administrative, and accountability purposes.

b. (U) Data from non-federal sources: These data sources are queried remotely, and only the results of the query are ingested into the FTTTF data mart for analysis.

c. (U) Analytical Notes and Annotations: The data mart contains annotations, notes, and draft reports composed by analysts reviewing data. The notes and annotations are intermediate outputs, not in final format and not ready for dissemination. They are stored in shared folders within the data mart and are accessible to other users.

(U) Disposition: DELETE/DESTROY when superseded by updated information or when no longer needed for analytical purposes, not to exceed the life of the system.

3. (U) Outputs: FTTTF users may obtain responses or "hits" that provide information useful to a current investigation or intelligence gathering activity.

a. (U) Queries: Using a web browser, users can search for subjects in a variety of datasets or take an existing dataset and batch match it against other datasets. The search

results are recorded within the data mart and are used to trace back and determine what information was known at a given point in time.

(U) Disposition: DELETE/DESTROY 99 years after the date of the query.

b. (U) Investigative Leads: Leads and other information that are used for investigative or intelligence purposes are incorporated into the related FBI investigative or intelligence case file.

(U) Disposition: RETAIN/DESTROY commensurate with the retention period approved for the related file classification.

c. (U) E-mail notifications: Whenever new data is imported into the data mart that matches an existing search query, an e-mail notification is sent to the analysts' external email accounts.

(U) Disposition: Incorporate e-mails pertinent to ongoing investigations/intelligence gathering efforts into the related case file.

(U) DELETE/DESTROY electronic versions of the e-mail within 90 days.

4. (U) System Documentation: Specifications, design criteria, codebooks, record layouts, user guides, search tools and their dates of usage, change management requests, data dictionaries, and related information.

(U) Disposition: DELETE/DESTROY when superseded or obsolete, or upon authorized deletion of the related data set.

(U) Related Records:

5. (U) Policy, Usage Agreements, and Memoranda of Understanding:

(U) Disposition: DELETE/DESTROY when superseded or obsolete or upon termination of the FTTTF Datamart, whichever is sooner.

6. (U) Audit Records: The audit log contains information such as the date and time of record entries and updates, system inquiries, etc.

(U) Disposition: DELETE/DESTROY when 25 years old.

7. (U) Backups: Backups are maintained for potential system/server restoration in the event of a system/server failure or other unintentional loss of data.

(U) Disposition: DELETE/DESTROY/OVERWRITE incremental backup media when superseded by a full backup or when 90 days old.

(U) Disposition: DELETE/DESTROY/OVERWRITE full backup media when one year old.